REMARKS

Claims 117 to 136, 139 to 144, 146 to 165 and 168 to 174 are pending in this application; of which, claims 117 and 146 are the independent claims. No claims are yet allowed. Claims 117 to 136, 139 to 144, 146 to 165 and 168-174 are rejected. Claims 117, 119, 121, 122, 146, 148, 150 and 151 are amended herein. Favorable reconsideration and further examination are respectfully requested.

Before discussing the rejections set forth in the Office Action, Applicants had a teleconference with the Examiner which took place on Monday, 16 October 2006 to discuss the § 103 rejection. As a result of these discussions with the Examiner, the Examiner has indicated that Applicants' arguments below would overcome the §103 rejection if Applicants amended the claims to include that a transition represents "a type of vulnerability." The Examiner also indicated that allowability of the claims would depend on further search and consideration.

Claims 117 to 128, 130 to 136, 139 to 144, 146 to 157, 159 to 165 and 168 to 174 were rejected under 35 U.S.C. § 103(a) as being anticipated by Cohen et al. (U.S. Patent Number 6,952,779 referred to hereinafter as "Cohen") in view of Swiler et al ("Computer-Attack Graph Generation Tool" referred to hereinafter as "Swiler").

Amended claim 117 is directed to a method which includes using a computer to generate a pruned attack tree. Using the computer includes designating a root node of the pruned attack tree. The root node represents a starting point of an attack. Using the computer also includes, for a current node included in the pruned attack tree, connecting a resulting node having a first

state, representing a first host and access to the first host, and an edge, having a first transition value corresponding to one of a plurality of vulnerability types, to the current node if determined that another edge, having a second transition value corresponding to one of the plurality of vulnerability types, does not connect an ancestor of the current node to another node having a second state equivalent to the first state and the second transition value is equal to the first transition value.

The applied art is not understood to disclose or to suggest the foregoing features of claim 1. In particular, neither Cohen nor Swiler disclose or suggest that using the computer includes, for a current node included in the pruned attack tree, connecting a resulting node having a first state, representing a first host and access to the first host, and an edge, having a first transition value corresponding to one of a plurality of vulnerability types, to the current node if determined that another edge, having a second transition value corresponding to one of the plurality of vulnerability types, does not connect an ancestor of the current node to another node having a second state equivalent to the first state and the second transition value is equal to the first transition value.

As indicated by the Examiner, Cohen does not disclose or suggest a pruned attack tree much less generating a pruned attack tree (see page 3 of the Office Action). Therefore, Cohen does not disclose or suggest that that using the computer includes, for a current node included in the pruned attack tree, connecting a resulting node having a first state, representing a first host and access to the first host, and an edge, having a first transition value corresponding to one of a plurality of vulnerability types, to the current node if determined that another edge, having a

second transition value corresponding to one of the plurality of vulnerability types, does not connect an ancestor of the current node to another node having a second state equivalent to the first state and the second transition value is equal to the first transition value.

The Examiner uses the Swiler reference to make-up for the deficiency in Cohen of not generating a pruned attack tree. Swiler discloses pruning an attack graph; however, Swiler does not describe pruning an attack tree by using nodes and edges of an attack tree as claimed by Applicants. For example, Swiler does not include edges representing a "transition value corresponding to one of a plurality of vulnerability types." Rather, Swiler discloses that "a vulnerability refers to a state attribute" which are represented as nodes (see page 316 column 2 of Swiler). In particular, FIGS. 7 to 9 of Swiler each represents an attack graph on a single machine 1 using vulnerability nodes not edges. In one instance, Swiler references generating a vulnerability node, its ancestor vulnerabilities nodes, and their ancestor vulnerabilities nodes (see page 318, column 1 of Swiler).

Also, Applicants have amended claim 117 to indicate that a first state represents "a first host and access to the first host." On the other hand, in FIG. 7 of Swiler, Swiler shows eight nodes representing vulnerabilities on a single machine 1 whereas Applicants would show a single node. The differences defining nodes and edges between Applicants and Swiler in using edges and nodes is evident, for example, in the different use of notation. For example, letter A represents vulnerability A in Swiler (see page 316 column 2 of Swiler) whereas the letter A used in Applicants' specification indicates a state representing a host A and access to the host A.

Furthermore, even if Swiler's nodes did not represent vulnerabilities and were the same as Applicants' nodes, Swiler teaches that paths leading to C-B-D are essentially the same as B-C-D or D-B-C (see page 316, column 2 of Swiler). Thus, Swiler's method of pruning in effect includes less nodes (See FIGS. 7 and 9) than what Applicants' method as recited in claim 117 would include. This is because Swiler represents each transition from one node to another node as being the same type of transition. Applicants on the other hand have clearly distinguished a "transition value corresponding to one of a plurality of vulnerability types." For example, in FIG. 13 of Applicants' specification, the prune attack tree 600 includes a node 554 (state B) having a level 2 type vulnerability and a node 558 (state B) having a level 1 type vulnerability. Under Swiler's method of pruning both node 558 and node 554 would not coexist in the pruned attack graph. Therefore, Swiler does not disclose or suggest that that using the computer includes, for a current node included in the pruned attack tree, connecting a resulting node having a first state, representing a first host and access to the first host, and an edge, having a first transition value corresponding to one of a plurality of vulnerability types, to the current node if determined that another edge, having a second transition value corresponding to one of the plurality of vulnerability types, does not connect an ancestor of the current node to another node having a second state equivalent to the first state and the second transition value is equal to the first transition value.

Even if Cohen and Swiler were combined, the hypothetical combination would not disclose or suggest that using the computer includes, for a current node included in the pruned attack tree, connecting a resulting node having a first state, representing a first host and access to

the first host, and an edge, having a first transition value corresponding to one of a plurality of vulnerability types, to the current node if determined that another edge, having a second transition value corresponding to one of the plurality of vulnerability types, does not connect an ancestor of the current node to another node having a second state equivalent to the first state and the second transition value is equal to the first transition value. For at least the foregoing reasons, Applicants submit that the Swiler and Cohen references should be withdrawn with respect to claim 117.

Claim 146 is an article claim having corresponding features to claim 117. Applicants submit that the Cohen and Swiler references should also be withdrawn with respect to claim 146 for at least the same reasons as claim 117.

Applicants submit that all dependent claims now depend on allowable independent claims.

For at least the foregoing reasons, Applicants request withdrawal of the art rejection.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for withdrawing the prior art cited with regards to any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicants submit that the entire application is now in condition for allowance. Such action is respectfully requested at the Examiner's earliest convenience.

All correspondence should be directed to the address below. Applicants' attorney can be reached by telephone at (781) 401-9988 ext. 23.

No fee is believed to be due for this Response; however, if any fees are due, please apply such fees to Deposit Account No. 50-0845 referencing Attorney Docket: MIT-186PUS.

Respectfully submitted,

Date: 19 October 2006

Anthony T. Moosey
Reg. No. 55,773

Daly, Crowley, Mofford & Durkee, LLP
354A Turnpike Street - Suite 301A
Canton, MA 02021-2714
Telephone: (781) 401-9988 ext. 23
Facsimile: (781) 401-9966